Benutzerhandbuch - Deutsch

FUJITSU Software ServerView Suite

# ServerView Blade System Integration Pack für MS System Center Operations Manager

Version 6.0

Ausgabe Februar 2015

## Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

## Zertifizierte Dokumentation nach DIN EN ISO 9001:2008

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2008 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

## Copyright und Handelsmarken

Copyright © 2015 Fujitsu Technology Solutions GmbH.

Alle Rechte vorbehalten.
Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

# Inhalt


**1 Einleitung . . . . . 5**

**1.1 Zielgruppen und Zielsetzung . . . . . 6**
**1.2 ServerView Suite Link-Sammlung . . . . . 6**
**1.3 Dokumentation zur ServerView Suite . . . . . 8**
**1.4 Darstellungsmittel . . . . . 8**
**1.5 Abkürzungen . . . . . 9**

**2 Integrationsvoraussetzungen . . . . . 11**

**3 Installation, Konfiguration und Deinstallation . . . . . 13**

**3.1 ServerView Integration installieren . . . . . 13**
**3.2 Blade System Monitor Service installieren . . . . . 14**
3.2.1 Installierte Dateien . . . . . 14
3.2.2 Konfiguration des Blade System Monitor Service . . . . . 15
**3.3 Management Pack installieren . . . . . 18**
3.3.1 Installierte Dateien . . . . . 18
3.3.2 Import des Management Packs . . . . . 19
**3.4 SNMP-Trap-Konfiguration . . . . . 19**
3.4.1 SNMP-Trap-Konfiguration testen (optional) . . . . . 21
**3.5 ServerView Integration deinstallieren . . . . . 22**
3.5.1 Blade System Monitor Service deinstallieren . . . . . 22
3.5.2 Management Pack-Dateien deinstallieren . . . . . 23

**4 Eigenschaften der ServerView Integration in SCOM . . . . 25**

**4.1 Ermittlung und Überwachung der Blade System Monitor Services . . . . . 25**
**4.2 Ermittlung und Überwachung der Blade System-Gehäuse . 26**
**4.3 Ansichten . . . . . 26**

4.3.1 Ansicht Active Alerts . . . . . 27
4.3.2 Ansicht Blade Devices State . . . . . 28
4.3.3 Ansicht Components Health State . . . . . 28
4.3.4 Ansicht Enclosure State . . . . . 29
4.3.5 Ansicht Monitor Service State . . . . . 29
4.3.6 Monitore . . . . . 29

**4.4 Fujitsu Blade System-Gehäuseaufgaben . . . . . 31**
4.4.1 Computer-Management-Konsole . . . . . 31
4.4.2 ServerView Operations Manager (Serverliste) . . . . . 31
4.4.3 ServerView Remote Management . . . . . 33

**4.5 SNMP-Traps, -Ereignisse und -Alarme . . . . . 33**

**4.6 Wissensdatenbank . . . . . 34**

**5 Arbeiten mit der ServerView Integration in SCOM . . . . . 35**

**5.1 Konfiguration - Einstellungen für die Überwachung außer Kraft setzen . . . . . 35**
5.1.1 Ändern der Einstellungen (Beispiel: Überwachung von Blade System Fan Subsystem) . . . . . 35
5.1.2 Vorsichtsmaßnahmen beim Außerkraftsetzen der Einstellungen für das Überwachungsintervall . . . . . 37
5.1.2.1 Paarweise Änderung von Integritäts- und Überwachungsmonitoren . . . . . 37
5.1.2.2 Empfohlene Werte für den IntervalSeconds-Parameter . . . . 38
5.1.2.3 Außerkraftsetzung zugehöriger Parameter des Überwachungsmonitors . . . . . 38

**5.2 Konfiguration - Alarme aktivieren und deaktivieren . . . . . 39**

**5.3 Konfiguration - Zeiteinstellung für Objektermittlung ändern . 41**

**6 Anhang . . . . . 43**

**6.1 Log-Dateien anlegen . . . . . 43**
6.1.1 Ermittlungs- und Überwachungs-Log-Dateien . . . . . 43
6.1.2 Blade System Monitor Service Log-Dateien . . . . . 45

# 1 Einleitung

Die PRIMERGY ServerView Suite von Fujitsu Technology Solutions bietet zahlreiche ServerView-Integrationsmodule, mit denen sich PRIMERGY Systeme und die Management-Software ServerView Operations Manager auf einfache Art und Weise in andere Enterprise Management-Systeme integrieren lassen.

Dieses Handbuch beschreibt Version 6.0 des Fujitsu Software ServerView Blade System Integration Pack for MS SCOM, mit dem PRIMERGY Blade Systeme in Microsoft System Center Operations Manager 2012 (SCOM 2012) integriert werden können.

Mithilfe des Fujitsu Software ServerView Blade System Integration Pack for MS SCOM lassen sich PRIMERGY Blade Systeme von Fujitsu Technology Solutions über SCOM überwachen. Die Überwachung eines PRIMERGY Blade Systems wird insbesondere durch Monitore von Hardware- und Software-Komponenten realisiert und durch Symbole angezeigt.

Wenn der MMB im Blade-Chassis Fehler bei der Überwachung der Blade-Chassis-Hardware und -Firmware entdeckt, werden diese Fehler an den *Fujitsu PRIMERGY Blade System Monitor Service* als SNMP-Traps weitergeleitet. Der *Fujitsu PRIMERGY Blade System Monitor Service* (im Folgenden als *Blade System Monitor Service* bezeichnet) schreibt diese Fehler auf dem lokalen System als Einträge in das Ereignisprotokoll *FujitsuBladeSystemMMB*. SCOM überprüft die Einträge des Ereignisprotokolls anhand vordefinierter Regeln und zeigt diese als Warnungen auf der SCOM-Konsole an.

Darüber hinaus können Regeln angewendet werden, die beim Auftreten eines Fehlers eine entsprechende Aktion auslösen, z. B. das Senden einer E-Mail mit Fehlerbeschreibung an den Hardware-Support.

## 1.1 Zielgruppen und Zielsetzung

Das vorliegende Handbuch wendet sich an Systemverwalter, Netzverwalter und Service-Fachleute, die über fundierte Kenntnisse zu Hardware, Software und ServerView Operations Manager verfügen. Desgleichen werden solide Grundkenntnisse des Microsoft System Center Operations Manager vorausgesetzt.

## 1.2 ServerView Suite Link-Sammlung

Fujitsu Technology Solutions stellt Ihnen über die Link-Sammlung zahlreiche Downloads und weiterführende Informationen zur ServerView Suite und zu PRIMERGY Servern zur Verfügung.

Zur ServerView Suite werden Ihnen Links zu folgenden Themen angeboten:

- Forum
- Service Desk
- Handbücher
- Produktinformationen
- Sicherheitsinformationen
- Software Downloads
- Schulungen

Die Downloads umfassen u. a.:

- aktuelle Software-Stände zur ServerView Suite sowie ergänzende Readme-Dateien.
- Informationsdateien und Aktualisierungsdateien (Update Sets) für systemnahe Software-Komponenten (BIOS, Firmware, Treiber, ServerView-Agenten und ServerView-Update-Agenten) zur Aktualisierung der PRIMERGY Server anhand des ServerView Update Managers oder für den lokalen Update einzelner Server anhand des ServerView Update Managers Express.
- die aktuellen Versionen aller Dokumentationen zur ServerView Suite

Die Downloads können kostenlos vom Fujitsu Technology Solutions Web-Server heruntergeladen werden.

Zu PRIMERGY Servern werden Ihnen Links zu folgenden Themen angeboten:

- Service Desk
- Handbücher
- Produktinformationen
- Ersatzteilkatalog

### Zugriff auf die ServerView Link-Sammlung

Die Link-Sammlung der ServerView Suite erreichen Sie über verschiedene Wege:

1. über den ServerView Operations Manager

   ► Wählen Sie auf der Startseite bzw. in der Menüzeile*Help – Links* aus.

   Anschließend wird die Startseite der Link-Sammlung angezeigt.

2. über die Startseite der Online-Dokumentation zur ServerView Suite auf dem Manual-Server von Fujitsu Technology Solutions.

   Sie gelangen auf die Startseite der Online-Dokumentation mit folgendem Link:

   *http://manuals.ts.fujitsu.com*

   ► Wählen Sie links in der Auswahlliste *x86 Servers*.

   ► Klicken Sie rechts unter *Ausgewählte Dokumente* auf *PRIMERGY ServerView Links*.

   Anschließend wird die Startseite der ServerView Link-Sammlung angezeigt.

3. über die ServerView Suite DVD.

   ► Markieren Sie im Startfenster der ServerView Suite DVD die Option *ServerView Software Produktauswahl*.

   ► Klicken Sie auf *Starten*. Sie gelangen auf die Seite mit den Software-Produkten der ServerView Suite.

   ► Wählen Sie in der Menüleiste *Links*.

   Anschließend wird die Startseite der Link-Sammlung angezeigt.

## 1.3 Dokumentation zur ServerView Suite

Die Dokumentation ist über das Internet als Download kostenlos erhältlich. Die Online-Dokumentation zur ServerView Suite finden Sie unter *http://manuals.ts.fujitsu.com* und dem Link *x86 Servers*.

Einen Überblick über die Dokumentation, die Sie unter *ServerView Suite* finden, sowie die Ablagestruktur können Sie der ServerView Suite Sitemap (*ServerView Suite - Site Overview*).

## 1.4 Darstellungsmittel

| | |
|---|---|
| **Warnung** | Mit diesem Symbol wird auf Gefahren hingewiesen, die zu Gesundheitsgefährdung, Datenverlust und Geräteschäden führen können. |
| | Mit diesem Symbol werden wichtige Informationen und Tipps hervorgehoben. |
| *Kursive Schrift* | Im Fließtext werden Kommandos, Menüpunkte, Namen von Schaltflächen, Optionen, Variablen, Dateinamen und Pfadnamen kursiv dargestellt. |

### Bildschirmausgaben

Beachten Sie bitte, dass die Bildschirmausgaben teilweise systemabhängig sind und deshalb nicht in allen Details mit der Ausgabe auf Ihrem System übereinstimmen müssen. Ebenso können bezüglich der verfügbaren Menüpunkte systembedingte Abweichungen auftreten.

## 1.5 Abkürzungen

Die folgenden Abkürzungen werden im gesamten Manual verwendet:

| | |
|---|---|
| MP | Management Pack |
| SCE | Microsoft System Center Essentials |
| SCOM | (Microsoft) System Center Operations Manager |
| SNMP | Simple Network Management Protocol |

# 2 Integrationsvoraussetzungen

Die im Folgenden aufgeführten Voraussetzungen müssen für die Integration erfüllt sein.

**Management-Station**

Microsoft System Center Operations Manager 2012 (R2)

**Proxy-Server**

Für das Fujitsu Blade System Integration Pack muss der *Fujitsu PRIMERGY Blade System Monitor Service* auf einem oder mehreren Servern mit Windows-Betriebssystem installiert sein. Der *Blade System Monitor Service* wird für den Zugriff auf die verwalteten Blade Systeme seitens des System Center Operations Manager benötigt.

Der Einfachheit halber werden in diesem Dokument Server, auf denen der *Blade System Monitor Service* installiert ist, als „Proxy-Server“ bezeichnet. Jeder beliebige Server kann als Proxy-Server fungieren, sofern folgende Bedingungen erfüllt sind:

– Windows Server 2008 (x64) oder Windows Server 2008 R2 oder Windows Server 2012 oder Windows Server 2012 R2 ist installiert.

– Der SNMP-Dienst ist aktiviert.

– Der SCOM-Agent ist installiert.

**Verwaltete PRIMERGY Server**

Fujitsu PRIMERGY Blade System (BX400, BX600, BX900)

# 3 Installation, Konfiguration und Deinstallation

## 3.1 ServerView Integration installieren

Das Installationspaket befindet sich auf der ServerView Suite DVD unter *SVSSoftware/Software/Integration_Solutions/SCOM_BL* oder als Download auf der Webseite *http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/*.

Navigieren Sie auf der Webseite zum Ordner *ServerView/Integrations Lösungen* und suchen Sie das Paket *ServerView Blade System Integration Pack for Microsoft System Center Operations Manager 2012 and 2012 R22*. Laden Sie das Paket herunter und extrahieren Sie die *ZIP*-Datei in einen geeigneten Ordner.

Das Software-Paket enthält folgende Dateien:

– *Blade System Monitor Service 64 bit.exe*

– *SVISCOM-BL.exe*

– *Readme_en.pdf*

– *Readme_jp.pdf*

– *THIRDPARTYLICENSEREADME.txt*

Das Software-Paket enthält zwei zu installierende Bestandteile:

– Den *Fujitsu PRIMERGY Blade System Monitor Service*, der auf einem oder mehreren Proxy-Servern ausgeführt wird.

– Das *Fujitsu PRIMERGY Blade System Management Pack*, das auf dem Management-Server installiert und dann in SCOM importiert werden muss.

# 3.2 Blade System Monitor Service installieren

Starten Sie das Installationsprogramm *Blade System Monitor Service 64 bit.exe* und befolgen Sie die während des Installationsprozesses angezeigten Anweisungen.

## 3.2.1 Installierte Dateien

Standard-Installationspfad auf dem Proxy-Server:

*%ProgramFiles(x86)%\Fujitsu\ServerView Suite\SCOM Integration\SVISCOM-BL\MonitorService*

| **Ordner** | **Dateien** |
|---|---|
| Installationsordner | *BladeLogMsg.dll*<br>*converter.vbs*<br>*log4cplusU.dll*<br>*PRIMERGYBladeSystemMonitor.exe*<br>*PRIMERGYBladeSystemSNMP.dll*<br>*Readme_en.pdf* |
| *comm*-Unterordner | *ManagedPRIMERGYBlades.xml* |
| *config*-Unterordner | *PRIMERGYBladeSystemConfigSNMP.xml*<br>*PRIMERGYBladeSystemConfigSNMP.xsd*<br>*S31.traps* |
| *log*-Unterordner | *FujitsuBladeSystemMMB.log* |
| *Misc*-Unterordner | *eula_en.pdf*<br>*eula_jp_V2.pdf* |
| *SelectBlades*-Unterordner | *AddBladeEnclosureToSCOM.exe*<br>*AddBladeEnclosureToSCOM.exe.config* |

Tabelle 1: Installation des Blade System Monitor Service: Standard-Installationspfad

Das Installationsprogramm kopiert die erforderlichen Dateien (siehe Tabelle oben) und installiert und startet den *Blade System Monitor Service*.

## 3.2.2 Konfiguration des Blade System Monitor Service

Nach der Installation des *Blade System Monitor Service* aus dem Software-Paket starten Sie das Tool *AddBladeEnclosureToSCOM.exe*:

– In Windows Server 2008 finden Sie dieses Programm unter:

*Start -> Alle Programme -> Fujitsu -> ServerView Suite*

– In Windows Server 2012 finden Sie dieses Programm unter:

*Apps -> Fujitsu*

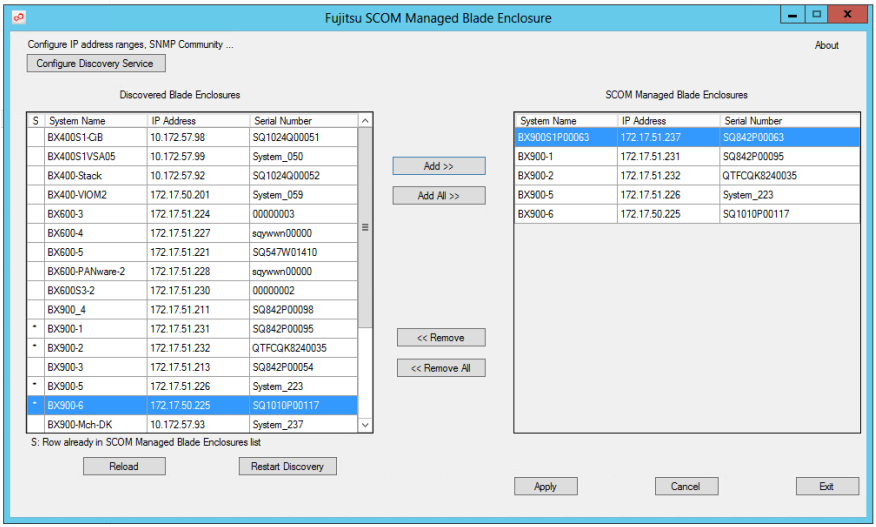


Bild 1: Konfiguration des Discovery Service

Sobald die GUI gestartet wurde, können Sie die gewünschten IP-Bereiche und Communitys konfigurieren, indem Sie in der oberen linken Ecke auf *Configure Discovery Service* klicken.

Hierdurch wird das Dialogfeld *Configure PRIMERGY Blade Server Monitor* geöffnet, in dem Sie verschiedene Suchschlüssel angeben können.

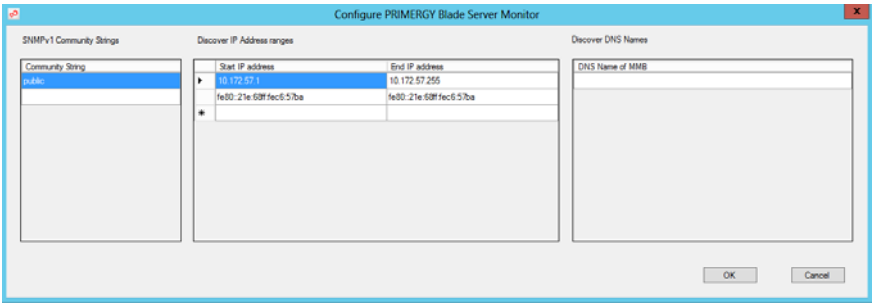


Bild 2: PRIMERGY Blade Server Monitor konfigurieren

*SNMPv1 Community Strings*

Ermöglicht die Konfiguration von SNMP-Community-Strings.

*Discover IP Address ranges*

Ermöglicht die Festlegung von IPv4- und IPv6-Adressbereichen, um Fujitsu PRIMERGY-Blade-Systeme zu finden.

Wenn nur die *Start-IP-Adresse* konfiguriert ist, wird diese einzige Adresse ermittelt.

*Discover DNS Names*

Ermöglicht die Konfiguration von MMB DNS-Namen, um die DNS-Namen für Fujitsu PRIMERGY-Blade-Systeme zu ermitteln.

- Klicken Sie auf *OK*, um die Einstellungen zu übernehmen.

Wenn die Konfiguration abgeschlossen ist, klicken Sie auf *Restart Discovery*.

**Beachten Sie:**

Für IP-Bereiche mit mehr als 256 zu überprüfenden IP-Adressen nimmt die Ermittlung etwas Zeit in Anspruch.

Sobald die Ermittlung abgeschlossen ist, sollten in der linken Tabelle Einträge zu sehen sein:

- Um ein zu überwachendes Blade System auszuwählen, klicken Sie auf den entsprechenden Eintrag und dann auf *Add*, um den Eintrag in die rechte Tabelle zu verschieben.
- Um ein Blade System aus der Überwachung zu entfernen, wählen Sie den entsprechenden Eintrag in der rechten Tabelle aus und klicken dann auf *Remove*.

- Klicken Sie auf *Apply*, um alle in der rechten Tabelle angezeigten Blade Systeme zu überwachen.

Jetzt können Sie das Management Pack installieren und importieren. (Siehe Abschnitt "Management Pack installieren" auf Seite 18.)

# 3.3 Management Pack installieren

Starten Sie das Installationsprogramm *SVISCOM-BL.exe* auf dem System, auf dem die SCOM-Konsole installiert ist, und befolgen Sie die während des Installationsprozesses angezeigten Anweisungen.

## 3.3.1 Installierte Dateien

Der Standard-Installationspfad auf der Management-Station lautet folgendermaßen:

*%ProgramFiles(x86)%\Fujitsu\ServerView Suite\SCOM Integration\SVISCOM-BL*

| Ordner | Dateien |
|---|---|
| Installationsordner | *eula_en.pdf*<br>*Fujitsu.PRIMERGY.BladeSystem.mp*<br>*PRIMERGYBladeSystemEventsSCOM_en.pdf*<br>*Readme_en.pdf*<br>*StartServerViewS2.exe*<br>*SVISCOM-BL.Log.ini* |

Tabelle 2: Installation des Management Packs: Standard-Installationspfad

Nach Abschluss der Installation müssen Sie die SCOM-Konsole neu starten, um die Umgebungsvariablen zu aktivieren, die von den Konsolenaufgaben verwendet werden (siehe Abschnitt "Fujitsu Blade System-Gehäuseaufgaben" auf Seite 31).

Wenn eine oder mehrere SCOM-Konsolen auf anderen Computern als der Management-Station installiert werden und Sie die ServerView Operations Manager-Konsolenaufgabe verwenden möchten, installieren Sie das Management Pack auf diesen Computern ebenfalls (siehe Abschnitt "ServerView Operations Manager (Serverliste)" auf Seite 31).

### 3.3.2 Import des Management Packs

Verwenden Sie die SCOM-Konsole, um die Datei *Fujitsu.PRIMERGY.BladeSystem.mp* in üblicher Weise aus folgendem Ordner zu importieren:

*%ProgramFiles(x86)%\Fujitsu\ServerView Suite\SCOM Integration\SVISCOM-BL*

Zum Importieren der Management Packs benötigen Sie SCOM-Administratorrechte.

## 3.4 SNMP-Trap-Konfiguration

Damit die MMBs der Blade Systeme Alarme von den Blade Systemen empfangen können, müssen die MMBs für das Senden von Traps an den Proxy-Server konfiguriert sein, auf dem das Blade System als *SCOM Managed Blade Enclosure* konfiguriert ist.

Auf allen Proxy-Servern muss der SNMP-Trap-Dienst ausgeführt werden.

Damit die SNMP-Traps vom MMB zum Proxy-Server gelangen können, muss am MMB das Trap Forwarding aktiviert sein.

Im Folgenden wird beschrieben, wie der SNMP-Trap-Dienst über die MMB-Web-Oberfläche konfiguriert wird. Weitere Informationen finden Sie im Benutzerhandbuch zum entsprechenden PRIMERGY Blade System.

Gehen Sie wie folgt vor:

1. Melden Sie sich am MMB des zu überwachenden Blade Systems an und wechseln Sie zu den Einstellungen für SNMP:

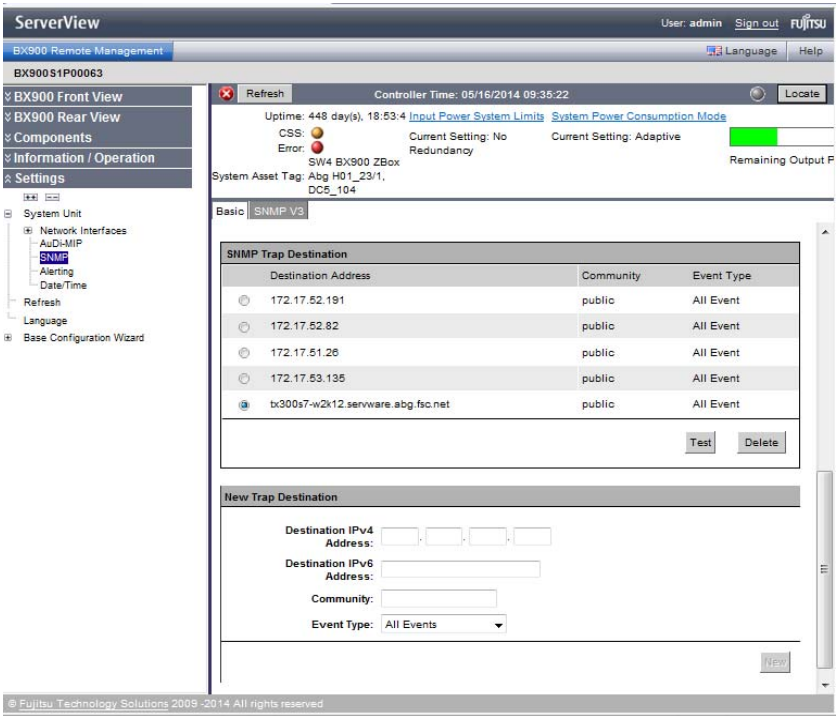


Bild 3: Konfiguration des SNMP-Trap-Dienstes

2. Geben Sie unter *Ziel-IPv4-Adresse* die IP-Adresse (IPv4) oder den FQDN (Fully Qualified Domain Name) eines Proxy-Servers als neues Trap-Ziel an.

Obwohl der SNMP-Trap-Dienst alle Traps empfängt, werden nur Traps mit der Gewichtung *CRITICAL* oder *MAJOR* im Management Pack aktiviert. Alle Traps mit der Gewichtung *MINOR* werden zwar implementiert, im Management Pack jedoch deaktiviert. Sie können im Bereich *Konfiguration* der SCOM-Konsole aktiviert werden (siehe Abschnitt "SNMP-Traps, -Ereignisse und -Alarme" auf Seite 33).

### 3.4.1 SNMP-Trap-Konfiguration testen (optional)

Sie haben die Möglichkeit, die Trap-Kommunikation zwischen einem MMB und dem Proxy-Server zu testen.

Gehen Sie wie folgt vor:

1. Melden Sie sich am MMB des zu überwachenden Blade Systems an und wechseln Sie zu den Konfigurationseinstellungen für SNMP (siehe Seite 20).
2. Wählen Sie im Bereich *SNMP Trap Destination* den Proxy-Server aus, dessen Kommunikation getestet werden soll.
3. Klicken Sie auf *Test*.
4. Öffnen Sie den *Server-Manager* auf dem ausgewählten Proxy-Server und öffnen Sie das Tool *Computerverwaltung*.
5. Navigieren Sie zur *Ereignisanzeige* und erweitern Sie den Ordner *Anwendungs- und Dienstprotokolle*:

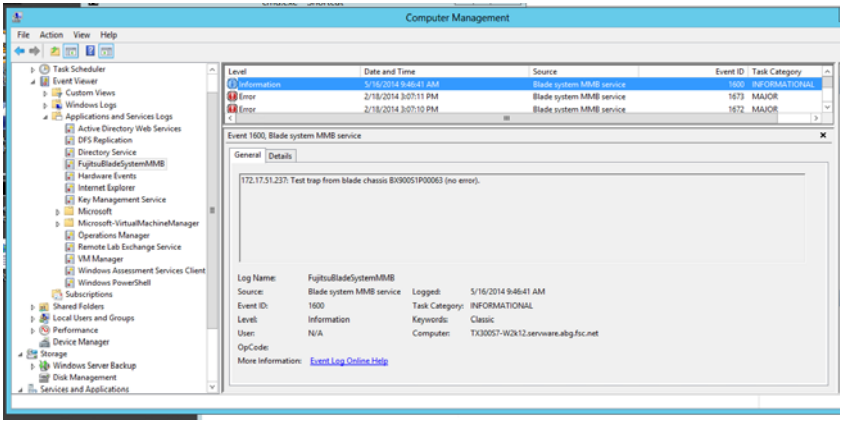


Bild 4: Anwendungs- und Dienstprotokolle

6. Wählen Sie das Protokoll *FujitsuBladeSystemMMB*.
7. Suchen Sie nach einem Protokolleintrag mit *Level* = "Information", *Event ID* = "1600" und *Source* = "Blade system MMB service".

   Wenn solch ein Eintrag vorhanden ist, weist dies darauf hin, dass die Kommunikation zwischen dem MMB und dem Proxy-Server erfolgreich getestet wurde.

# 3.5 ServerView Integration deinstallieren

Um Alarme in SCOM zu vermeiden, wird die folgende Vorgehensweise empfohlen:

1. Starten Sie den *Wartungsmodus für Fujitsu Blade System Enclosures* im Bereich *Überwachung* der SCOM-Konsole:
2. Löschen Sie das Fujitsu PRIMERGY Blade System MP im Bereich *Verwaltung* der SCOM-Konsole.

   Zum Löschen der Management Packs benötigen Sie SCOM-Administratorrechte.
3. Deinstallieren Sie den *Blade System Monitor Service* (siehe Abschnitt "Blade System Monitor Service deinstallieren" auf Seite 22).
4. Deinstallieren Sie die Management Pack-Dateien (siehe Abschnitt "Management Pack-Dateien deinstallieren" auf Seite 23).

## 3.5.1 Blade System Monitor Service deinstallieren

Die Deinstallation der ServerView Integration können Sie auf zwei Arten durchführen:

– Ausführen des Windows-Deinstallationsprogramms auf dem/den Proxy-Server(n):

  Rufen Sie in der Systemsteuerung über *Programme hinzufügen oder entfernen* oder über *Programme und Funktionen* die installierten Programme auf. Der folgende Eintrag wird angezeigt:

  *Fujitsu ServerView Blade System Monitoring Service (64 bit)*

  Hier können Sie den *Blade System Monitor Service* deinstallieren.

– Erneutes Aufrufen des Installationsprogramms *Blade System Monitor Service 64 bit.exe*:

  Starten Sie das Installationsprogramm wie bei der Installation und deinstallieren Sie dann den *Blade System Monitor Service*.

### 3.5.2 Management Pack-Dateien deinstallieren

Die Deinstallation des Management Packs können Sie auf zwei Arten durchführen:

– Ausführen des Windows-Deinstallationsprogramms auf der Management-Station:

  Rufen Sie in der Systemsteuerung über *Programme hinzufügen oder entfernen* oder über *Programme und Funktionen* die installierten Programme auf. Der folgende Eintrag wird angezeigt:

  *Fujitsu ServerView Blade System Integration Pack for MS SCOM*

  Sie können hier das Management Pack deinstallieren.

– Erneutes Aufrufen des Programms *SVISCOM-BL.exe*.

  Starten Sie das Installationsprogramm *SVISCOM-BL.exe* wie bei der Installation und deinstallieren Sie dann das Integration Pack.

Wenn der Deinstallationsprozess abgeschlossen ist, sind alle Registry-Einträge vom Server entfernt. Einige Unterverzeichnisse und Dateien verbleiben im Installationsverzeichnis. Sie können sie manuell löschen.

# 4 Eigenschaften der ServerView Integration in SCOM

Das Management Pack Fujitsu PRIMERGY Blade System enthält die Definitionen für die SCOM Integration. Der Dateiname dieses Pakets lautet *Fujitsu.PRIMERGY.BladeSystem.mp*.

## 4.1 Ermittlung und Überwachung der Blade System Monitor Services

Ein *Blade System Monitor Service* wird ermittelt, wenn beide der folgenden Bedingungen erfüllt sind:

– Der *Blade System Monitor Service* ist auf einem Windows-Server installiert (Proxy-Server, siehe Abschnitt "Blade System Monitor Service installieren" auf Seite 14) und dieser Server wurde zum SCOM-Management hinzugefügt (SCOM-Agent auf dem zu überwachenden Server installiert). Dies wird in der Ansicht *Windows-Computer* angezeigt.

– Der *Blade System Monitor Service* hat die korrekte Version (6.0.x.x).

Wenn ein *Blade System Monitor Service* ermittelt wird, wird dieser in der Ansicht *Monitor Service State* angezeigt (siehe Abschnitt "Ansicht Monitor Service State" auf Seite 29).

## 4.2 Ermittlung und Überwachung der Blade System-Gehäuse

Zur Ermittlung von Blade System-Gehäusen und deren Komponenten sind folgende Schritte erforderlich:

1. Definieren Sie mithilfe des Auswahl-Tools *AddBladeEnclosureToSCOM.exe* eine Liste von Blade System-Gehäusen, die verwaltet werden sollen (siehe Abschnitt "Konfiguration des Blade System Monitor Service" auf Seite 15). Die Liste verwalteter Blade System-Gehäuse wird in der rechten Spalte des Auswahl-Tool-Fensters angezeigt.
2. Wenn das Management Pack importiert wird, werden die zu verwaltenden Blade System-Gehäuse automatisch von SCOM ermittelt.

## 4.3 Ansichten

Durch die Integration des Management Packs wird ein Verzeichnis *Fujitsu Blade System Enclosures* im Bereich *Überwachung* der SCOM-Konsole erstellt. In diesem Verzeichnis werden die im Folgenden beschriebenen Ansichten angezeigt:

- *Active Alerts*
- *Blade Devices State*
- *Components Health State*
- *Enclosure State*
- *Monitor Service State*

Der Integritätszustand in allen Ansichten wird durch die üblichen Symbole im Operations Manager dargestellt.

### 4.3.1 Ansicht Active Alerts

Die Ansicht *Active Alerts* zeigt alle Alarme, die dem Management Pack *Fujitsu PRIMERGY Blade System* zugeordnet sind und die den Auflösungsstatus *New* haben.

Folgende Ursachen können einen Alarm auslösen:

- Wenn ein überwachtes Blade System oder eine Blade System-Komponente sich in einem kritischen Integritätsstatus befindet.

  Dieser Alarm ist „selbstauflösend“, d. h. sobald die Ursache beseitigt ist, wird der Alarm wieder aus der Ansicht entfernt.

- Ein Ereignis, für das eine Regel im Management Pack definiert ist, ist in das Windows-Ereignisprotokoll eines Proxy-Servers geschrieben worden. Das Ereignis kann in den folgenden Windows-Protokollen angezeigt werden:

  – Anwendungs- und Dienstprotokolle/FujitsuBladeSystemMMB

  – Microsoft/Operations Manager-Ereignisprotokoll

  Diese Alarme werden weiterhin angezeigt, bis sie explizit geschlossen werden.

Eine Übersicht der Alarme, die durch Regeln aus Ereignissen erstellt werden, können Sie dem Dokument *PRIMERGYServerEventsSCOM_en.pdf* entnehmen, das dem Produkt beigelegt ist.

Alarme werden standardmäßig nur durch Ereignisse erzeugt, die mit der Gewichtung *Critical* (*Error*) in das Windows-Ereignisprotokoll (Operations Manager oder System) geschrieben worden sind. Ereignisse mit der Gewichtung *Warning* können auch angezeigt werden, wenn sie durch den Benutzer aktiviert werden (siehe Abschnitt "Konfiguration - Alarme aktivieren und deaktivieren" auf Seite 39).

### 4.3.2 Ansicht Blade Devices State

Die Ansicht *Blade Devices State* zeigt den Integritätsstatus aller Server Blades und Storage Blades in einem Blade System-Gehäuse an. Die Server Blades und Storage Blades aller verwalteten Blade System-Gehäuse werden in dieser Ansicht angezeigt.

Die Eigenschaften eines ausgewählten Server Blades oder Storage Blades werden in einem Fenster unterhalb dieser Ansicht angezeigt (Ansicht *Detail*).

Anzeige bestimmter Aufgaben:

– ServerView Operations Manager
– ServerView Remote Manager

Näheres hierzu finden Sie im Abschnitt "Fujitsu Blade System-Gehäuseaufgaben" auf Seite 31.

### 4.3.3 Ansicht Components Health State

Die Ansicht *Components Health State* zeigt den Integritätsstatus aller Komponenten-Subsysteme in einem Blade System-Gehäuse an. Im Einzelnen wird der Integritätsstatus folgender Komponenten-Subsysteme angezeigt:

– Stromversorgungseinheiten
– Lüftereinheiten
– Management Blade-Einheiten
– Temperatur-Sensoren
– Verbindungseinheiten
– KVM-Einheiten

Der Integritätsstatus der Komponenten-Subsysteme aller verwalteten Gehäuse wird in dieser Ansicht angezeigt.

Die Eigenschaften eines ausgewählten Komponententyps werden in einem Fenster unterhalb dieser Ansicht angezeigt (Ansicht *Detail*).

Anzeige bestimmter Aufgaben:

– ServerView Operations Manager
– ServerView Remote Manager

Näheres hierzu finden Sie im Abschnitt "Fujitsu Blade System-Gehäuseaufgaben" auf Seite 31.

### 4.3.4 Ansicht Enclosure State

In der Ansicht *Enclosure State* wird der allgemeine Integritätsstatus aller Gehäuse angezeigt.

Die Eigenschaften eines ausgewählten Gehäuses werden in einem Fenster unterhalb dieser Ansicht angezeigt (Ansicht *Detail*).

Wenn in der Ansicht *Detail* in den Eigenschaften *System Contact* oder *System Location* nicht druckbare Zeichen oder Unicode-Zeichen enthalten sind, wird die jeweilige Eigenschaft nicht korrekt angezeigt.

Anzeige bestimmter Aufgaben:

- ServerView Operations Manager
- ServerView Remote Manager

Näheres hierzu finden Sie im Abschnitt "Fujitsu Blade System-Gehäuseaufgaben" auf Seite 31.

### 4.3.5 Ansicht Monitor Service State

In der Ansicht *Monitor Service State* wird der Integritätsstatus der *Blade System Monitor Services* angezeigt, die auf den Proxy-Servern ausgeführt werden.

Die Eigenschaften des auf einem ausgewählten Server ausgeführten *Blade System Monitor Service* werden in einem Fenster unterhalb dieser Ansicht angezeigt (Ansicht *Detail*).

### 4.3.6 Monitore

Der in der Ansicht *Enclosure State* und in der Ansicht *Monitor Service State* angezeigte Integritätsstatus zeigt den aktuellen Integritätsstatus der überwachten Objekte wie Fujitsu PRIMERGY-Blade-Systeme oder Überwachungsdienste an (siehe Abschnitt "Ansicht Enclosure State" auf Seite 29 und Abschnitt "Ansicht Monitor Service State" auf Seite 29). Der Integritätsstatus wird in allen Fällen über eine Monitorhierarchie bestimmt, wobei der Integritätsstatus der einzelnen Monitore einen bestimmten Aspekt des Zustands der überwachten Objekte anzeigt. Die Monitore werden nicht nur zur Auswertung des allgemeinen Integritätsstatus eines Blade-Systems verwendet, sondern können auch zur Fehleranalyse herangezogen werden.

*Beispiel*

Wenn der allgemeine Zustand eines Blade-Systems einen Fehler anzeigt, wird der Fehlerstatus in der Ansicht *Enclosure State* angezeigt. Durch Auswahl des betroffenen Blade-Systems und Klicken auf *Health Explorer* wird der SCOM-Integritäts-Explorer geöffnet und ein Auszug der Monitorhierarchie angezeigt. Standardmäßig sind dabei nur die Monitore enthalten, die einen niedrigen Integritätsstatus an den allgemeinen Integritätsstatus weitergeben. Es ist deshalb möglich, die Weitergabe eines Fehlerstatus vom Gesamtstatus des Blade-Systems zu den Komponenten zurückzuverfolgen, die den Fehler verursacht haben (siehe nachfolgende Abbildung).

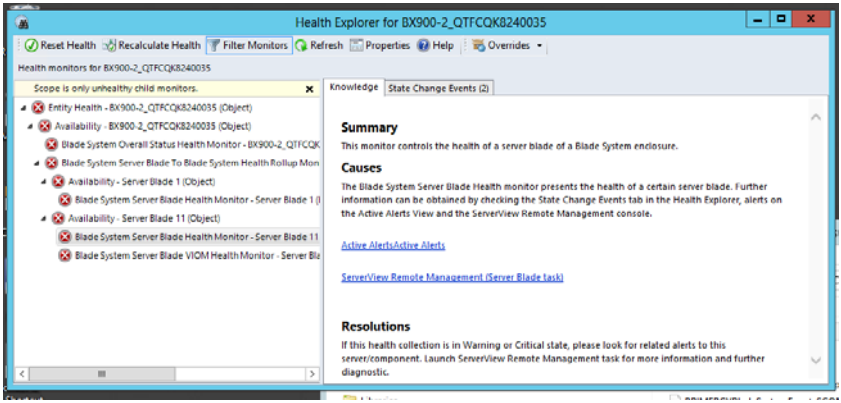
Health Explorer for BX900-2_QTFCQK8240035
Reset Health
Recalculate Health
Filter Monitors
Refresh
Properties
Help
Overrides
Health monitors for BX900-2_QTFCQK8240035
Scope is only unhealthy child monitors.
Entity Health - BX900-2_QTFCQK8240035 (Object)
Availability - BX900-2_QTFCQK8240035 (Object)
Blade System Overall Status Health Monitor - BX900-2_QTFCQK
Blade System Server Blade To Blade System Health Rollup Mon
Availability - Server Blade 1 (Object)
Blade System Server Blade Health Monitor - Server Blade 1 (
Availability - Server Blade 11 (Object)
Blade System Server Blade Health Monitor - Server Blade 11
Blade System Server Blade VIOM Health Monitor - Server Bla
Knowledge
State Change Events (2)
Summary
This monitor controls the health of a server blade of a Blade System enclosure.
Causes
The Blade System Server Blade Health monitor presents the health of a certain server blade. Further information can be obtained by checking the State Change Events tab in the Health Explorer, alerts on the Active Alerts View and the ServerView Remote Management console.
Active AlertsActive Alerts
ServerView Remote Management (Server Blade task)
Resolutions
If this health collection is in Warning or Critical state, please look for related alerts to this server/component. Launch ServerView Remote Management task for more information and further diagnostic.

Bild 5: Weitergabe eines Fehlerstatus zurückverfolgen

Das ServerView Blade System Integration Pack enthält zahlreiche Monitore, die nicht nur den Integritätsstatus der Zielobjekte modellieren, sondern auch den Integritätsstatus des Überwachungssystems selbst anzeigen. Sie werden deshalb benachrichtigt, wenn eine Komponente des Überwachungssystems ausfällt, weil in diesem Fall der Integritätsstatus des überwachten Blade-Systems oder einzelner Teile davon nicht mehr ausgewertet werden kann. Die Monitore, die den Integritätsstatus des Überwachungssystems anzeigen, werden hier "Überwachungsmonitore" genannt. Diese Monitore bilden ihre eigenen Monitorhierarchien. Ein Fehler des Überwachungssystems wirkt sich sowohl auf den Gesamtstatus von *Monitor Service* als auch auf den Gesamtstatus von *Enclosures* aus (siehe Abschnitt "Ansicht Monitor Service State" auf Seite 29 and Abschnitt "Ansicht Enclosure State" auf Seite 29).

# 4.4 Fujitsu Blade System-Gehäuseaufgaben

Aufgaben sind Aktionen, die im Aktionsbereich der SCOM-Konsole angezeigt werden. Welche Aufgaben angezeigt werden, hängt davon ab, welche Ansicht ausgewählt ist und welcher Eintrag in dieser Ansicht markiert ist. Die folgenden Aufgaben stehen zur Verfügung:

– Computer-Management-Konsole
– ServerView Operations Manager
– ServerView Remote Manager

## 4.4.1 Computer-Management-Konsole

Mit dieser Aufgabe wird die Microsoft Management Console (MMC-Anwendung) gestartet und der Zugriff auf die Daten des markierten PRIMERGY Servers ermöglicht.

## 4.4.2 ServerView Operations Manager (Serverliste)

Mit dieser Aufgabe wird der ServerView Operations Manager gestartet, um die Liste aller vom ServerView Operations Manager verwalteten Server (Serverliste) anzuzeigen.

Beim ersten Start der Software wird ein Dialogfeld angezeigt, das den Namen des Servers abfragt, auf dem ServerView Operations Manager installiert ist (siehe unten).

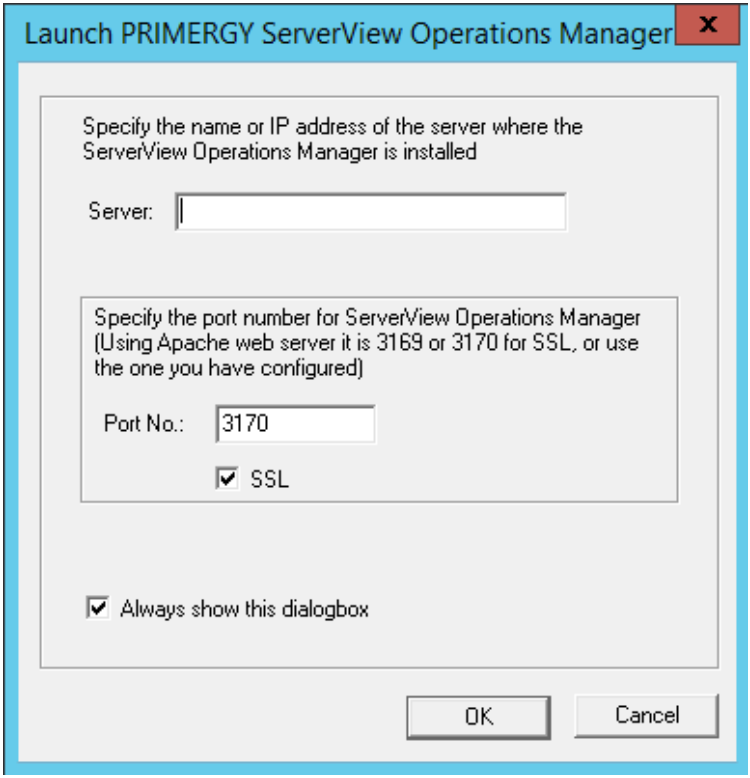
Launch PRIMERGY ServerView Operations Manager
Specify the name or IP address of the server where the ServerView Operations Manager is installed
Server:
Specify the port number for ServerView Operations Manager (Using Apache web server it is 3169 or 3170 for SSL, or use the one you have configured)
Port No.:
3170
SSL
Always show this dialogbox
OK
Cancel

Bild 6: Dialogfeld „Launch PRIMERGY ServerView Operations Manager“

Das Dialogfeld wird angezeigt, solange die Option *Always show this dialogbox* ausgewählt ist.

Wenn das Dialogfeld nicht mehr angezeigt wird und die Adresse oder die Anmeldeinformationen von ServerView Operations Manager sich geändert haben, verwenden Sie einen Texteditor, um die Datei *SVOMStart.ini* im Unterordner *ini* des Installationsverzeichnisses zu öffnen. Setzen Sie den Wert der Variable *Dialog*, die dem entsprechenden Server zugeordnet ist, von "no" auf "yes".

Wenn Sie die Adresse und die Portnummer der Operations Manager Management-Station eingegeben haben und auf *OK* klicken, wird ServerView Operations Manager gestartet.

ServerView Operations Manager fordert Sie auf, sich beim ServerView Suite Central Authentication Service anzumelden. Erst nach der erfolgreichen Anmeldung wird die Serverliste angezeigt.

### 4.4.3 ServerView Remote Management

Diese Aufgabe wird verwendet, um die Konsole der MMB-Web-Oberfläche mithilfe ihrer IPv4-Adresse (sofern verfügbar) aufzurufen.

Dies funktioniert nur, wenn der HTTPS-Port mit der Standard-Portnummer 443 für HTTPS-Ports konfiguriert ist.

## 4.5 SNMP-Traps, -Ereignisse und -Alarme

Wie in Abschnitt "SNMP-Trap-Konfiguration" auf Seite 19 beschrieben sendet das MMB eines Blade Systems SNMP-Traps an einen Proxy-Server. Der *Blade System Monitor Service* konvertiert die SNMP-Traps in Ereignisse, die im Ereignisprotokoll *FujitsuBladeSystem* des Proxy-Servers angezeigt werden.

Im Fujitsu ServerView Blade System Integration Pack sind Regeln für Ereignisse definiert, die einen Alarm hervorrufen. Die Alarme bleiben so lange in der Ansicht *Active Alerts* sichtbar, bis sie explizit geschlossen werden, d. h., bis ihnen der Auflösungsstatus *Closed*

zugewiesen wird. Ereignisse und Alarme sind unabhängig von Monitoren und haben keinen Einfluss auf den Status des Servers. Sie dienen nur zur Anzeige eines Ereignisses.

Eine Übersicht der integrierten Ereignisse können Sie der Datei *PRIMERGYServerEventsSCOM_en.pdf* entnehmen, die Sie im Installationsordner finden.

Es sind nur Ereignisse integriert, die die Gewichtung *Warning* oder *Critical* haben.

- Ein SNMP-Trap mit der Gewichtung *Critical* oder *Major* wird einem Windows-Ereignis mit der Gewichtung *Critical* zugeordnet.
- Ein SNMP-Trap mit der Gewichtung *Minor* wird einem Windows-Ereignis mit der Gewichtung *Warning* zugeordnet.

### Aktivierung/Deaktivierung von Alarmen

Per Voreinstellung erzeugen alle Ereignisse mit der Gewichtung *Critical* einen Alarm und alle Ereignisse mit der Gewichtung *Warning* erzeugen keinen Alarm. Sie können diese Standardeinstellungen im Bereich *Konfiguration* der SCOM-Konsole überschreiben. Die Überschreibung muss danach in einem beschreibbaren Management Pack gespeichert werden.

## 4.6 Wissensdatenbank

Zu den Ereignissen und Alarmen ist eine Wissensdatenbank (Knowledge Base) vorhanden. Je nach Art des Alarms werden bei Auftreten eines Fehlers verschiedene Lösungen/Aktionen angezeigt. Diese Lösungen finden Sie auch in der Datei *PRIMERGYServerEventsSCOM_en.pdf* in der letzten Spalte der aufgeführten Ereignisse.

# 5 Arbeiten mit der ServerView Integration in SCOM

## 5.1 Konfiguration - Einstellungen für die Überwachung außer Kraft setzen

Für die folgenden Subsysteme und Komponenten der Blade Systeme können Überwachungseinstellungen bis zu einem gewissen Grad geändert werden:

- Blade System Connection Subsystem
- Blade System Enclosure
- Blade System Enclosure Monitor Service
- Blade System Enclosure Server Blade
- Blade System Enclosure Storage Blade
- Blade System Fan Subsystem
- Blade System KVM Subsystem
- Blade System MMB Subsystem
- Blade System Connection Subsystem
- Blade System Temperature Sensors

### 5.1.1 Ändern der Einstellungen (Beispiel: Überwachung von Blade System Fan Subsystem)

Gehen Sie wie folgt vor:

1. Starten Sie die SCOM-Konsole.
2. Wählen Sie im Navigationsfenster des Bereichs *Konfiguration* das Verzeichnis *Management Pack-Objekte -> Monitore* aus.

   Im rechten Fenster werden daraufhin alle verfügbaren Monitore angezeigt.
3. Navigieren Sie zum Eintrag *Blade System Fan Subsystem* und erweitern Sie ihn. Erweitern Sie anschließend zunächst den Eintrag *Entity Health* und dann darunter den Eintrag *Availability*.

   Die Einträge sind alphabetisch sortiert. Um die Anzahl der angezeigten Einträge zu reduzieren, können Sie auch die Suchfunktion verwenden.

4. Doppelklicken Sie auf *Blade System Fan Health Monitor*, um das Dialogfeld mit den Einstellungen des Monitors zu öffnen.
5. Klicken Sie in der Registerkarte *Außerkraftsetzungen* dieses Dialogfelds auf *Außerkraftsetzung...* und wählen Sie *Für alle Objekte der Klasse: Blade System Fan Subsystem*.

   Das Dialogfeld *Außerkraftsetzungseigenschaften* mit den zu ändernden Eigenschaften wird geöffnet.
6. Zum Ändern einer Eigenschaft gehen Sie wie folgt vor:

   a) Wählen Sie die Eigenschaft in der Spalte *Außerkraftsetzung* aus.

   b) Ändern Sie den Wert der Option in der Spalte *Außerkraftsetzungswert*.

   Bei der Lüfterüberwachung können Sie folgende Parameter außer Kraft setzen:

| **Parametername** | **Außerkraftsetzungswert** |
|---|---|
| Warnung bei Status | Der Monitor befindet sich in einem kritischen Integritätsstatus. /Der Monitor befindet sich in einem kritischen oder Warnungsintegritätsstatus. |
| Warnungspriorität | Hoch / Mittel / Niedrig |
| Warnungsschweregrad | Kritisch / Informationen / Warnung / Wie Monitorintegrität |
| Warnung automatische Auflösung | Wahr / Falsch |
| Aktiviert | Wahr / Falsch |
| Generiert Warnungen | Wahr / Falsch |
| IntervalSeconds | Zeitintervall (in Sekunden), in dem der Monitor die Komponente überwacht. |

Tabelle 3: Überwachungsparameter für Blade System Fan Subsystem

Die Außerkraftsetzungen müssen in einem nicht-schreibgeschützten Management Pack gespeichert werden. Microsoft empfiehlt, dazu nicht das *Standard-Management Pack* zu verwenden. Über die Schaltfläche *Neu* können Sie sich ein neues Management Pack erstellen.

Es wird empfohlen, zuerst das Management Pack zu wählen, in dem die Außerkraftsetzung gespeichert werden soll.

7. Klicken Sie auf *OK*, um die Einstellungen im ausgewählten Management Pack zu speichern. Das Dialogfeld wird geschlossen.
8. Klicken Sie im anschließend angezeigten Dialogfeld für den Monitor auf *Schließen*, um die Konfiguration der Einstellungen zu beenden.

## 5.1.2 Vorsichtsmaßnahmen beim Außerkraftsetzen der Einstellungen für das Überwachungsintervall

Der Parameter *IntervalSeconds* bestimmt das Zeitintervall des SCOM-Überwachungszyklus (siehe Tabelle 3 auf Seite 36). Der Parameterwert ist für die Überwachung von Blade System-Gehäusen optimiert.

Normalerweise ist eine Anpassung dieses Werts nicht erforderlich. Es wird dringend empfohlen, den Parameter *IntervalSeconds* nicht zu ändern. Wenn eine Änderung des Parameters *IntervalSeconds* jedoch unabdingbar ist, sollten die unten beschriebenen Vorsichtsmaßnahmen getroffen werden.

### 5.1.2.1 Paarweise Änderung von Integritäts- und Überwachungsmonitoren

Die Blade System-Subsysteme und Blade System-Komponenten werden von einem Monitor-Paar überwacht:

– Der <*subsystem*> *Health Monitor* gibt den Status des überwachten Subsystems oder der überwachten Komponente an.

– Der <*subsystem*> *Monitoring Monitor* gibt an, ob die Überwachung selbst fehlerfrei funktioniert.

Wenn der Parameter *IntervalSeconds* geändert wird, muss er sowohl auf dem Integritätsmonitor als auch auf dem Überwachungsmonitor eines Blade System-Subsystems oder einer Blade System-Komponente geändert werden. Der Parameterwert *IntervalSeconds* muss stets für beide Monitortypen identisch sein.

#### 5.1.2.2 Empfohlene Werte für den IntervalSeconds-Parameter

Der Standardwert von *IntervalSeconds* ist 360 Sekunden. Wenn dieser Wert überhaupt geändert wird, sollte er nur erhöht werden.

Überwachungsintervalle von weniger als 360 Sekunden sollten unbedingt vermieden werden.

#### 5.1.2.3 Außerkraftsetzung zugehöriger Parameter des Überwachungsmonitors

Die Außerkraftsetzungsparameter *IntervalSeconds*, *ConsolidatorCount* und *ConsolidatorTimeWindow* hängen miteinander zusammen und sollten nicht einzeln geändert werden. Wenn einer dieser Parameter geändert wird, sollten die übrigen Parameter ebenfalls so angepasst werden, dass die folgenden Bedingungen erfüllt sind:

– *ConsolidatorTimeWindow* = *IntervalSeconds* * *ConsolidatorCount* + 120

– *IntervalSeconds* ≥ 360

– *ConsolidatorCoun*t ≥ 2

## 5.2 Konfiguration - Alarme aktivieren und deaktivieren

Per Voreinstellung erzeugen alle Ereignisse mit der Gewichtung *Critical* einen Alarm und alle Ereignisse mit der Gewichtung *Warning* erzeugen keinen Alarm. Diese Voreinstellung können Sie außer Kraft setzen.

Jeder Alarm kann über seinen Titel und seine *Ereignis-ID* in der Datei *PRIMERGYServerEventsSCOM_en.pdf* ermittelt werden, die detaillierte Informationen zu jedem Ereignis und zur Lösung des zugrunde liegenden Problems enthält.

Gehen Sie wie folgt vor:

1. Starten Sie die SCOM-Konsole.
2. Wählen Sie im Navigationsfenster des Bereichs *Konfiguration* das Verzeichnis *Management Pack-Objekte -> Regeln* aus. Im rechten Fenster werden dann alle Regel-Gruppen, die in SCOM definiert sind, angezeigt.
3. Wählen Sie die Gruppe *Blade System Enclosure Monitor Service* aus und klicken Sie danach auf den Alarm, der aktiviert oder deaktiviert werden soll.

   In der Spalte *Standardmäßig aktiviert* wird angezeigt, ob ein Alarm für das entsprechende Ereignis erzeugt wird (*Ja*) oder nicht (*Nein*). Nicht aktivierte Alarme sind auch durch das ausgegraute Symbol in der ersten Spalte zu erkennen.
4. Doppelklicken Sie auf den gewünschten Alarm. Ein Dialogfeld mit den Einstellungen wird geöffnet.
5. Wechseln Sie in diesem Dialogfeld zur Registerkarte *Außerkraftsetzungen*, klicken Sie auf *Außerkraftsetzung...* und wählen Sie *Für alle Objekte vom Typ: Blade System Enclosure Monitor Service* aus.

   Das Dialogfeld *Außerkraftsetzungseigenschaften* mit den zu ändernden Eigenschaften wird geöffnet.

6. Gehen Sie zum Aktivieren bzw. Deaktivieren des Alarms wie folgt vor:

   1. Wählen Sie in der Spalte *Außerkraftsetzung* den Parameter *Aktiviert* aus.
   2. Ändern Sie den Wert der Option in der Spalte *Außerkraftsetzungseinstellung* (*Falsch* → *Wahr* oder *Wahr* → *Falsch*).

   Die Außerkraftsetzungen müssen in einem nicht-schreibgeschützten Management Pack gespeichert werden. Microsoft empfiehlt, dazu nicht das *Standard-Management Pack* zu verwenden. Über die Schaltfläche *Neu* können Sie sich ein neues Management Pack erstellen.

7. Klicken Sie auf *OK*, um die Einstellungen im ausgewählten Management Pack zu speichern. Das Dialogfeld wird geschlossen.

8. Klicken Sie im anschließend angezeigten Dialogfeld für den Monitor auf *Schließen*, um die Konfiguration der Einstellungen zu beenden.

Entsprechend können Sie Alarme für einzelne Server aktivieren oder deaktivieren. Wählen Sie in diesem Fall *Für ein bestimmtes Objekt der Klasse: Blade System Enclosure Monitor Service* anstatt *Für alle Objekte der Klasse: Blade System Enclosure Monitor Service* aus. Anschließend können Sie den/die gewünschten Proxy-Server auswählen und wie oben beschrieben fortfahren.

## 5.3 Konfiguration - Zeiteinstellung für Objektermittlung ändern

Das Zeitintervall für die Ermittlung von Komponenten von Blade System-Gehäusen ist voreingestellt.

Um diese Voreinstellung zu ändern, gehen Sie wie folgt vor:

1. Starten Sie die SCOM-Konsole.
2. Wählen Sie im Navigationsfenster des Bereichs *Konfiguration* das Verzeichnis *Management Pack-Objekte -> Objektermittlungen* aus. Im rechten Fenster werden daraufhin alle Ermittlungsregeln, die in SCOM definiert sind, angezeigt.
3. Wählen Sie im Fenster *Objektermittlungen* die Objektermittlung aus, die Sie ändern wollen.

   Für die Ermittlung von Blade System-Gehäusen ist dies die Gruppe *Ermittelter Typ: Blade System Enclosure* mit dem Eintrag *Blade System Enclosure Discovery Rule*.
4. Doppelklicken Sie auf den gewünschten Eintrag. Das Dialogfeld *Blade System Enclosure Discovery Rule Properties* wird geöffnet.
5. Wählen Sie die Registerkarte *Außerkraftsetzungen* aus und klicken Sie dort auf *Außerkraftsetzung...*.
6. Wählen Sie je nach vorzunehmender Änderung entweder *Für alle Objekte der Klasse: Blade System Enclosure Monitor Service* oder *Für ein bestimmtes Objekt der Klasse: Blade System Enclosure Monitor Service* aus:
   - Haben Sie *Für ein bestimmtes Objekt der Klasse: Blade System Enclosure Monitor Service* ausgewählt, wird die Außerkraftsetzung nur für einen bestimmten Proxy-Server ausgeführt.
   - Wenn Sie *Für alle Objekte der Klasse: Blade System Enclosure Monitors* auswählen, werden alle ermittelten Proxy-Server zur Auswahl angeboten. Wählen Sie die/den Proxy-Server aus und klicken Sie auf *OK*.

   *Im Dialogfeld Außerkraftsetzungseigenschaften* können Sie die gewünschte Außerkraftsetzung auswählen.

   Nach Empfehlung von Microsoft sollten Sie zum Speichern Ihrer Änderungen nicht das Standard-Management Pack verwenden.

7. Um das Zeitintervall für die Ermittlung zu ändern, wählen Sie den entsprechenden Eintrag in der Spalte *Außerkraftsetzung* aus.

   Sie können nur die Werte ändern, die in der Spalte *Außerkraftsetzungswert* Zahlen enthalten.

   Geben Sie den neuen Zeitraum (in Sekunden) für die Ermittlung in der Spalte *Außerkraftsetzungswert* ein (Parametername: *Fujitsu PRIMERGY BladeSystem Enclosure DiscoveryDataSource Interval Seconds*).

   Microsoft empfiehlt, für Ermittlungen keine Zeiträume von weniger als vier Stunden zu verwenden.

8. Klicken Sie auf *OK*, um die Einstellungen im ausgewählten Management Pack zu speichern. Das Dialogfeld wird geschlossen.

9. Klicken Sie im anschließend angezeigten Dialogfeld für den Monitor auf *OK*, um die Konfiguration der Einstellungen zu beenden.

# 6 Anhang

## 6.1 Log-Dateien anlegen

Für die Fehleranalyse können Log-Dateien des *SNMP Trap Sammel Dienstes* angelegt werden. Das Blade System Integration Pack stellt drei Arten von Log-Dateien zur Verfügung:

– Ermittlungs-Log-Dateien mit Debug-Informationen zum SCOM-Ermittlungsprozess

– Überwachungs-Log-Dateien mit Debug-Informationen zum SCOM-Überwachungsprozess

– *Blade System Monitor Service* -Log-Dateien mit vom Fujitsu PRIMERGY Blade System Monitor generierten Debug-Informationen

### 6.1.1 Ermittlungs- und Überwachungs-Log-Dateien

Ermittlungs- und Überwachungs-Logs werden über eine Initialisierungsdatei mit dem Namen *SVISCOM-BL.Log.ini* aktiviert. Diese Datei befindet sich im Installationsverzeichnis (siehe Abschnitt "Installierte Dateien" auf Seite 14).

Die Log-Dateien werden im Unterverzeichnis *SVISCOM\BL* des Verzeichnisses abgelegt, das in die Systemumgebungs-Variable *TEMP* eingetragen ist. In der Regel ist dies das Verzeichnis *C:\Windows\TEMP*. Dabei steht *C:* für die Systempartition.

Wenn das Unterverzeichnis *SVISCOM\BL* nicht vorhanden ist, gilt Folgendes: Für jede SCOM-Ermittlung wird eine Kopie der Initialisierungsdatei mit dem Namen *SVISCOM-BL.Log.in_* im Ordner *%TEMP%\SVSCOM* jedes Proxy-Servers generiert.

*SVISCOMLog.ini* enthält Debug-Optionen für alle Ermittlungs- und Überwachungsfunktionen des Management Packs. Die Option *DebugMode* definiert, ob die Überwachung für eine bestimmte Funktion aktiviert werden soll. Die Option *DebugLevel* definiert, wie detailliert die bereitgestellten Debug-Informationen sind.

Gehen Sie Im Fall einer Fehleranalyse wie folgt vor:

1. Benennen Sie die Datei *SVISCOMLog.in_* auf jedem Proxy-Server in *SVISCOMLog.ini* um.

2. Überprüfen Sie die Debug-Optionen für jede zu überwachende Funktion (Ermittlung und Überwachung) und setzen Sie sie auf den gewünschten Wert.

*Beispiel: Einstellungen in der Datei SVISCOM.BL.Log.ini*

```
[BladeSystemDiscovery]
DebugMode=yes
DebugLevel=15

[BladeComponentsMonitor]
DebugMode=yes
DebugLevel=15
```

Es werden je nach Wunsch die folgenden Log-Dateien angelegt:

- *PYBladeSystemDiscovery_<servername>.log*
- *PYBladeSystemMonitor_<enclosureserialnumber>_ConnectUnits.log*
- *PYBladeSystemMonitor_<enclosureserialnumber>_Enclosure.log*
- *PYBladeSystemMonitor_<enclosureserialnumber>_FanUnits.log*
- *PYBladeSystemMonitor_<enclosureserialnumber>_KVMUnits.log*
- *PYBladeSystemMonitor_<enclosureserialnumber>_MMBUnits.log*
- *PYBladeSystemMonitor_<enclosureserialnumber>_PowerSupplyUnits.log*
- *PYBladeSystemMonitor_<enclosureserialnumber>_ServerBlades.log*
- *PYBladeSystemMonitor_<enclosureserialnumber>_StorageBlades.log*
- *PYBladeSystemMonitor_<enclosureserialnumber>_TempSensors.log*

Diese Dateien sind für die weitere Analyse an den Fujitsu Support zu senden.

Soll das Anlegen von Log-Dateien wieder abgeschaltet werden, dann benennen Sie die Datei *SVISCOMLog.ini* um.

### Aktualität der Log-Dateien

Log-Dateien werden nur dann umgehend erzeugt, wenn die Initialisierungsdatei vorhanden ist und das Fujitsu Management Pack bereits importiert wurde. Wenn das Management Pack bereits importiert wurde, werden je nach den in den Ermittlungs- oder Überwachungsskripten festgelegten Ausführungsintervallen Log-Dateien erzeugt. Es kann deshalb bis zu 4 Stunden dauern, bis alle Log-Dateien erzeugt wurden.

### 6.1.2 Blade System Monitor Service Log-Dateien

Die Log-Dateien des *Blade System Monitor Service* werden im Unterverzeichnis *log* des Installationsordners von *Blade System Monitor Service* auf einem Proxy-Server gespeichert.

Standardmäßig werden in der Log-Datei des *Blade System Monitor Service* nur wenige Informationen gespeichert. Um erweiterte Log-Dateien des *Blade System Monitor Service* zu erstellen, können Sie die Konfigurationsdatei *PRIMERGYBladeSystemConfigSNMP.xml* anpassen. Diese Datei befindet sich im Unterverzeichnis *config* des Installationsordners von *Fujitsu PRIMERGY Blade System Monitor Service* (siehe Abschnitt "Installierte Dateien" auf Seite 14).

Um die Log-Dateien des *Blade System Monitor Service* anzupassen, gehen Sie wie folgt vor:

1. Editieren Sie die Datei *PRIMERGYBladeSystemConfigSNMP.xml* mit einem Texteditor (z. B. mit *Notepad*).

   Setzen Sie im Bereich *<LogFile> ... </LogFile>* den Wert `<Threshold><old_value></Threshold>` auf `<Threshold><new_value></Threshold>`, wobei einer der folgenden Werte verwendet werden muss:

   – ERROR
   – WARN (Dies ist die Voreinstellung)
   – INFO
   – TRACE

   Bei *INFO* erhalten Sie mehr Informationsmeldungen, bei *TRACE* zusätzliche DEBUG Ausgaben.

2. Starten Sie den *Fujitsu PRIMERGY Blade System Monitor Service* neu, damit die angepassten Werte in Kraft treten.

Um die Erstellung von Log-Dateien für den *Blade System Monitor Service* zu deaktivieren, setzen Sie den Wert *<Threshold><value></Threshold>* auf den ursprünglichen Wert *<Threshold>WARN</Threshold>WARN* zurück und starten den *Fujitsu PRIMERGY Blade System Monitor Service* neu.